



Defence Industry
Leadership Program

DILP

Research

Paper

Countering Adversarial Narratives

What can defence industry do to counter adversarial narratives in a contested informational environment?

Authors

Leith Biddell
Darren Campbell
Sam Fletcher
Michael Paay
Luca Talmesio

DEFENCE INDUSTRY COUNTERING ADVERSARIAL NARRATIVES

2023 Defence Industry Leadership Program

Concept Paper

Sam Fletcher

Michael Paay

Darren Campbell

Luca Talmesio

Leith Biddell



Executive Summary

Adversarial narratives have been used for centuries to discredit political adversaries, manipulate public opinion, and shape public policy. However, in recent years the rise of the internet has significantly increased this threat, with the advancement of AI expected to further impact this exponentially.

Adversarial narratives have the potential to have a negative influence on the growth, credibility, and stability of Defence Industry, and threaten Australia's political stability and national security.

Given this threat, this paper addresses the question of *What can the Defence Industry do to counter adversarial narratives in a contested informational environment?* The Research Project Team used a variety of research methodologies to explore this question, including case study analysis; in-depth desktop research and literature reviews; targeted questioning of AI programs such as *ChatGPT-4* and Google's *Bard*; and semi structured qualitative interviews with media thought leaders.

As a result of this research, the team found the threat of adversarial narratives was a real and immediate one that was not fully understood. To counter these, it is recommended:

- recognising and acknowledging the threat of adversarial narratives, with investment by Government and Industry into fully understanding the danger they pose.
- ensuring an understanding of the actors behind adversarial narratives to identify who they are, their capabilities and their intent.
- ensuring an understanding of the rapid emergence of the use of Cyber and AI by adversaries to influence opinion and target Government and Industry, as well as the potential opportunities of these mechanisms to counter and respond to the ongoing threat.
- supporting the preservation of trust in Australia's institutes by highlighting our sovereign skills, including openness and transparency from Government regarding Defence acquisitions to allow the Defence Industry to better demonstrate capability offerings.
- using the media to highlight the unique offerings of Defence Industry SMEs and proactively tell good news stories; actively promote brand marketing; and be on the front foot to enable visibility of counter narratives and achieve positive influence.
- supporting education, vigilance, and responsiveness to adversarial narratives by ensuring visibility and promotion of Cognitive Immunity training throughout the Defence Industry and Department of Defence. Industry advocacy organisations are encouraged to assist in providing this guidance, support, and education, with the Defence Industry also contributing through company policies and procedures, and investment.

Finally, the key recommendation of the Research Project Team is that the Defence Industry needs to collaborate and work with Academia and Government more broadly to seek a cohesive approach to this issue. It is also important that the Defence Industry has a common front, with Primes and SMEs encouraged to align media strategies and engagement, with the starting point being additional investment and recognition of the threat of AI through a series of dedicated conferences and summits.

Table of Contents

Executive Summary	2
About	4
Definitions.....	5
Introduction	6
AUKUS Case Study	10
Cyber Focus Area.....	18
AI Focus Area.....	21
Findings.....	25
Recommendations.....	27
Conclusion	29
References.....	30
Appendix 1	32
Appendix 2	33

About

Acknowledgements

The team would like to thank all the people who gave their time in support of this paper. The team would especially like to thank our Research Policy Adviser - Dr Sharon Mascall-Dare OAM, who provided her extensive expertise, encouraged us to go outside of our comfort zone, inspired us to think differently and came along with us on the journey every step of the way.

Disclaimer

The contents of this report are the opinions and conclusions of the authors and do not necessarily represent the views of the authors' organisations, the contributors, the contributors' organisations, the Defence Industry Leadership Program (DILP), or the Defence Teaming Centre (DTC).

Acronyms

Acronym	Explanation
ADF	Australian Defence Force
AFS	Australian Future Submarines
ASC	Australian Submarine Corporation
AUKUS	Australia, United Kingdom (UK), and United States (US) Trilateral Security Partnership
DOD	Department of Defence
DILP	Defence Industry Leadership Program
DTC	Defence Teaming Centre
GoA	Government of Australia
IE	Information Environment
IM	Information Manipulation
IW	Information Warfare
LoTE	Life of Type Extension
NPS	Nuclear Powered Submarines
SME	Small to Medium Enterprise

Definitions

Adversarial Narrative

Intentionally distributed adversarial narratives without a required chronology or sequence of web artefacts, and which seek to enrage and divide internet users¹ For the purposes of this paper, adversarial narratives are those on social media and traditional media and are accessible by the Australian public.

Misinformation

Information that is false but not intended to cause harm.²

Disinformation

Information that is false, however, is intended to manipulate and cause damage.³

Malinformation

Information that stems from the truth but is often exaggerated in a way that misleads and can cause harm.⁴

Information Warfare

Information Warfare is defined as the use and management of information to pursue a competitive advantage through both offensive and defensive efforts.⁵

Information Manipulation

Information Manipulation is defined as intent to shape public opinion or undermine trust in the authenticity of information, through using new and traditional media to amplify distrust and foment unrest.⁶

¹ Decker, B, 2019, *Adversarial Narratives: A New Model for Disinformation*; The Global Disinformation Index, <<https://www.disinformationindex.org/research/2019-4-1-adversarial-narratives-a-new-model-for-disinformation/>>

² *How to identify misinformation, disinformation and malinformation*, 2022, Canadian Centre for Cyber Security

³ *How to identify misinformation, disinformation and malinformation*, 2022, Canadian Centre for Cyber Security

⁴ *How to identify misinformation, disinformation and malinformation*, 2022, Canadian Centre for Cyber Security

⁵ Wilson, G, 2023, *Information Warfare: what is it, and why should we care*, <Information Warfare: what is it, and why should we care? | The Cove (army.gov.au)>

⁶ The Cybersecurity and Infrastructure Security Agency (CISA), *information_manipulation_infographic_508.pdf*

Introduction

Completion of a research project is a major component of the Defence Industry Leadership Program (DILP) which is designed to demonstrate the knowledge and tools learned by students throughout the program, and in turn provide a benefit to the industry. The authors of this paper constitute the 2023 DILP Project Team 4; for brevity, and to disambiguate their work from other researchers in the field of Information Warfare (IW), the authors will collectively be referred to as the 'Research Project Team' throughout this report.

The Research Project Team was initially allocated a research topic which focused on the Department of Defence (DOD) and Defence Industry's task in educating Australians on their role, as well as to consider how Defence Primes can, or cannot, respond to media reports.

The Research Project Team and the Research Policy Advisor discussed the initial topic and agreed it was too broad and had the risk of not achieving defined outcomes or recommendations which would benefit the Defence Industry. A variation to the research topic was proposed to, and approved by, the DTC training team which provided a more defined scope of research, and proved to have realistic outcomes which could benefit the Defence Industry.

Research Topic

What can the Defence Industry do to counter adversarial narratives in a contested information environment?

Research Approach

Due to the scope of the topic remaining quite broad, the Research Project Team undertook a literature review to understand the meaning of adversarial narratives and their impact on Government, Defence, and Defence Industry. The team also reviewed various case studies to investigate examples where such narratives have potentially shaped the direction of policy.

Following an analysis of this information, it was agreed that the AUKUS Security Partnership was the most appropriate case study to highlight the impact of adversarial narratives on Government and Defence Industry. Research was also undertaken regarding the Cyber and Artificial Intelligence (AI) domains, as the Research Project Team recognised that these areas had a direct impact on the future of adversarial narratives and were potential areas for opportunities or solutions.

Accordingly, in-depth desktop literature reviews of the AUKUS case study and the Cyber and AI focus areas were completed. These reviews focused on traditional media outlets; adversarial media; publications and media releases; Defence Industry media; and academic publications and papers.

Additional research was also undertaken to determine what the Defence Industry is currently doing to counter adversarial narratives.

During the literature review, the Research Project Team recognised the growing impact and importance of AI, and that the Information Environment (IE) was transforming at a rapid rate.

To test the potential of AI to generate opportunities or solutions to combat adversarial narratives, the team asked targeted questions of *ChatGPT-4* and Google's *Bard* programs. As AI is an emerging technology, these research methods were used to substantiate information gained through more traditional research methods.

Finally, semi-structured qualitative interviews were completed with media thought leaders to gain their insights into the current contested IE; potential ways to counter adversarial narratives; and to test the Research Project Team's analysis and early thinking in relation to the findings and proposed recommendations.

Background

The Research Project Team's first step was to examine why the research question is an important one to ask, why it needs to be asked now, and what the Defence Industry is currently doing about it.

Adversarial narratives can be categorised as follows: *misinformation* is false but not intended to cause harm; *disinformation*, is also false but is intended to manipulate and cause damage; and *malinformation* stems from the truth but is often exaggerated in a way that misleads and can cause harm.⁷ Terms also used in this report to describe misinformation, disinformation and malinformation include fake news, propaganda, and false and misleading content.

These types of narratives are not new, for example the term 'Fake News' was first used in the 1890s.⁸ The Human Rights Commissioner stated in August this year that 'misinformation has been spread for political gain since Octavian used fake news to discredit Mark Antony in ancient Rome.'⁹ However, the rise of the internet as a fundamental source of information has resulted in it becoming a very effective instrument for spreading false and misleading information with unprecedented speed and reach.¹⁰

Technological advances enable the creation of sophisticated false and misleading content, with mining of personal data enabling the coordination and direct targeting of this information. This is achieved through fake social media accounts which target those who may be more likely to accept and share a particular message.

⁷ *How to identify misinformation, disinformation and malinformation*, 2022, Canadian Centre for Cyber Security

⁸ *The Real Story of Fake News*, nd, Merriam-Webster

⁹ Human Rights Commissioner Lorraine Finlay, 2023, *Why Misinformation Bill risks Freedoms it Aims to Protec*, The Australian, published Thursday 24th August 2023

¹⁰ Leshner, M., H. Pawelec and A. Desai, 2022, *Disentangling untruths online: Creators, spreaders and how to stop them*, OECD Going Digital Toolkit Notes, No. 23, OECD Publishing, Paris

Once shared, recipients' friends are more likely to believe the misleading content as it appears to come from a trusted person; they then share it with their friends, who then are likely to share the information further through their networks and so on.¹¹

For example, Facebook is described in the *Understanding Mass Influence* report commissioned by the DOD as being a very efficient platform for the spread of misinformation and is susceptible to manipulation by malicious actors.¹²

In 2022 alone, Meta identified more than 400 Android and Apple apps which were designed to steal Facebook information; removed 5.8 billion fake accounts globally; and just in Australia, displayed fact check warnings on over 9 million distinct pieces of content.¹³

From an international perspective, the Organisation for Economic Cooperation and Development (OECD) believes the creation and dissemination of false and misleading information erodes the trust the public has in the integrity of the information it receives from the government and mainstream media, and 'undermines democratic norms, national security, and public order.'¹⁴

From a national perspective, the 2023 Edelman Trust Barometer found that only 36% of Australian respondents said they trusted journalists, and 48% believed the media were a source of false information.¹⁵

General Angus Campbell in his address to the 2023 Australian Strategic Policy Institute (ASPI) Conference, spoke about the erosion of trust in key institutions due to the increase in fake news on social media.

He warned that taken to their extremes, it [fake news] has 'the potential to fracture and fragment entire societies so that they no longer possess the collective will to resist an adversary's intentions...consequently, the aim of these operations is to change not only what people think, but how they think and act.'¹⁶

The Defence Industry plays an important role in supporting Australia's stability and security.¹⁷ Therefore, given the potential impact of adversarial narratives, an extensive literature review was undertaken across several sites and databases to see what contribution the industry was making in this area.

¹¹ Buckmaster L, Wils, T, nd, *Responding to fake news*, Parliament of Australia

¹² Ebbott, E, Saletta, M, Stearne, R, Webb, B, Dowling, M, Farina, M, Young, G, Job, P, 2021, *Understanding Mass Influence*, Edith Cowan University, Macquarie University, University of Adelaide, University of Melbourne, University of New South Wales

¹³ Meta 2023, *Meta response to the Australian disinformation and misinformation industry code – January – December 2022*

¹⁴ Leshner, M., H. Pawelec and A. Desai, 2022, *Disentangling untruths online: Creators, spreaders and how to stop them*, OECD Going Digital Toolkit Notes, No. 23, OECD Publishing, Paris

¹⁵ Edelman 2023, *Edelman Trust Barometer – Australian Report*

¹⁶ Hollingworth 2023, *ADF Chief warns of 'truth decay' in talk touching on AI and disinformation*, Defence Connect, 22 September 2023

¹⁷ Price, M, *Australia's Defense Industry Minister: The importance of AUKUS and a strong economy*, Defense News, 6 December 2021

A summary of these results is outlined at Figure 1 below:

SEARCH TERM INCL AUSTRALIAN DEFENCE INDUSTRY	GOOGLE SCHOLAR	GOOGLE	DEFENCE INDUSTRY WEBSITE (SEARCH)	DEFENCE INDUSTRY ANNUAL REPORTS/PLANS
Countering adversarial narratives	Nil	Nil	Nil	Nil
Misinformation	Nil	1	Nil	Nil
Disinformation	Nil	2	Nil	Nil
Malinformation	Nil	Nil	Nil	Nil
Fake news	Nil	Nil	Nil	Nil
Propaganda	Nil	Nil	Nil	Nil

Figure 1: Literature Review Outcomes

While it is acknowledged that some information on this topic may not be available in the public domain, it was surprising how little information was discovered.

From the information that was sourced, most of the results were articles or links relating to a University of Technology Senior Lecturer winning a 2023 Defence Industry Award for her work in this area. The other search results related to the DOD's IW Star Shot program.¹⁸

¹⁸ *Combating Disinformation through Collaborative Research*, Department of Defence Media Centre, 22nd December 2022, <<https://www.dst.defence.gov.au/news/2022/12/22/combating-disinformation-through-collaborative-research>>

AUKUS Case Study

The Research Project Team’s case study outlines how the AUKUS decision [to acquire Nuclear Powered Submarines] impacted the Australian Submarine Industry. The decision made by the Commonwealth Government triggered numerous media articles that were based on facts, but also contained a large degree of misinformation, disinformation and malinformation.

To demonstrate, the following case study uses several media articles discovered during the research phase as examples. The AUKUS case study provides perspective and context regarding the impact of adversarial narratives on the Australian Defence Industry.

Firstly however, understanding the chronology of the Australian submarine development path is paramount, and is depicted in Figure 2 below.

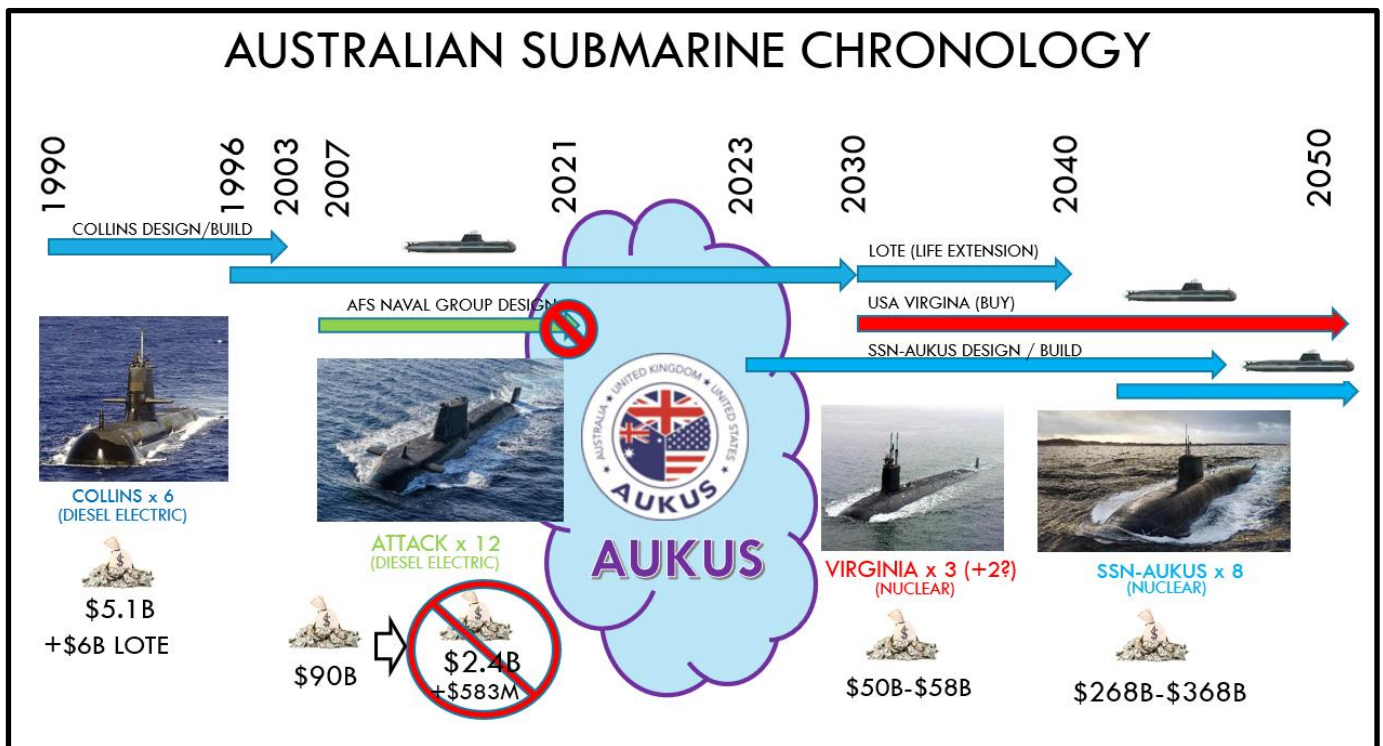


Figure 2: Australian Submarine Development

Collins Class

The *Collins* class submarines were the first submarines to be built in Australia and were constructed at Osborne, South Australia. This was a collaboration between Swedish company *Kockums* and the Australian Submarine Corporation (ASC); and based on a Swedish design.

The fleet consisted of six *Collins* class that were each named after significant RAN personnel who distinguished themselves during World War 2.

It was decreed that at least 60% of all construction was contributed to by Australian Industries, and after several years of design work, construction commenced on the first vessel which was named *Collins*. She was launched in 1996 and the final submarine was launched in 2003, with a total cost for design and construction of AUD5.1 billion, equating to AUD850 million for each submarine.

Australian Future Submarines (AFS)

The program to replace the *Collins* class with 12 *Attack* class submarines commenced in 2007 with plans to launch the first boat by 2025. In 2014 there were significant delays and in 2015 a competitive evaluation process began for construction between Japanese, French and German designs. In 2016, the Government of Australia (GoA) announced that the French Diesel-Electric submarine designed by *Naval Group* was awarded the contract. Work commenced and continued based on the expectation the submarines would be built at the ASC shipyards in South Australia. In 2020, the total anticipated cost was expected to be approximately AUD90 billion.

AUKUS – Virginia and SSN-AUKUS

In 2021, Prime Minister Scott Morrison announced the cancellation of the contract with *Naval Group* in conjunction with announcing the creation of the AUKUS Trilateral Security Partnership. Under AUKUS, the UK and US will assist Australia to acquire nuclear powered submarines (NPS). The pact also includes cooperation on advanced cyber mechanisms, AI and autonomy, quantum technologies, undersea capabilities, hypersonic and counter-hypersonic capabilities, electronic warfare innovation, and information sharing.

Cancelling the *Attack* class build saw a significant cost impact to both Government and Industry - the AFS program had already spent AUD2.4 billion and in addition, GoA paid *Naval Group* AUD538 million in compensation.

Under AUKUS, the proposal is for Australia to buy 3-5 *Virginia* class NPS from the US at a cost of between AUD50 billion and AUD58 billion, taking place between 2030 and 2050. Subsequently, Australia will build eight SSN-AUKUS NPS in collaboration with the UK and US. These are planned for construction in Adelaide but will use designs, components and sub-assemblies from the UK and US. The total cost is estimated to be between AUD268 billion and AUD368 billion, with the first submarine expected to be launched in the early 2040's.

Due to this plan generating a capability gap, it was necessary to create a Life of Type Extension (LoTE) for the *Collins* class. These Submarines were originally planned to operate until 2030 however, with the LoTE program, including significant upgrades, it is now expected to continue in service until approximately 2040, at a cost of AUD6 billion.

Media Reaction

The decision by GoA initiated an immediate and compelling response from the media, resulting in masses of media articles across multiple media platforms from numerous sources, making it nearly impossible to separate fact from fiction.

To understand the landscape of a contested IE, the Research Project Team conducted research and analysis surrounding misinformation, disinformation and malinformation specifically related to AUKUS and found excessive amounts of information and media articles. After a glance at the headlines, it was often difficult to separate fact from fiction, or to determine the true intent of an article. Researched articles were taken from several different viewpoints and often gave very different perspectives on the same information.

The Research Project Team conducted deep analysis to determine if relevant articles were attempting to portray misinformation, disinformation, and malinformation, or a combination of all three. Figure 3 below depicts several headlines the Research Project Team discovered and analysed.

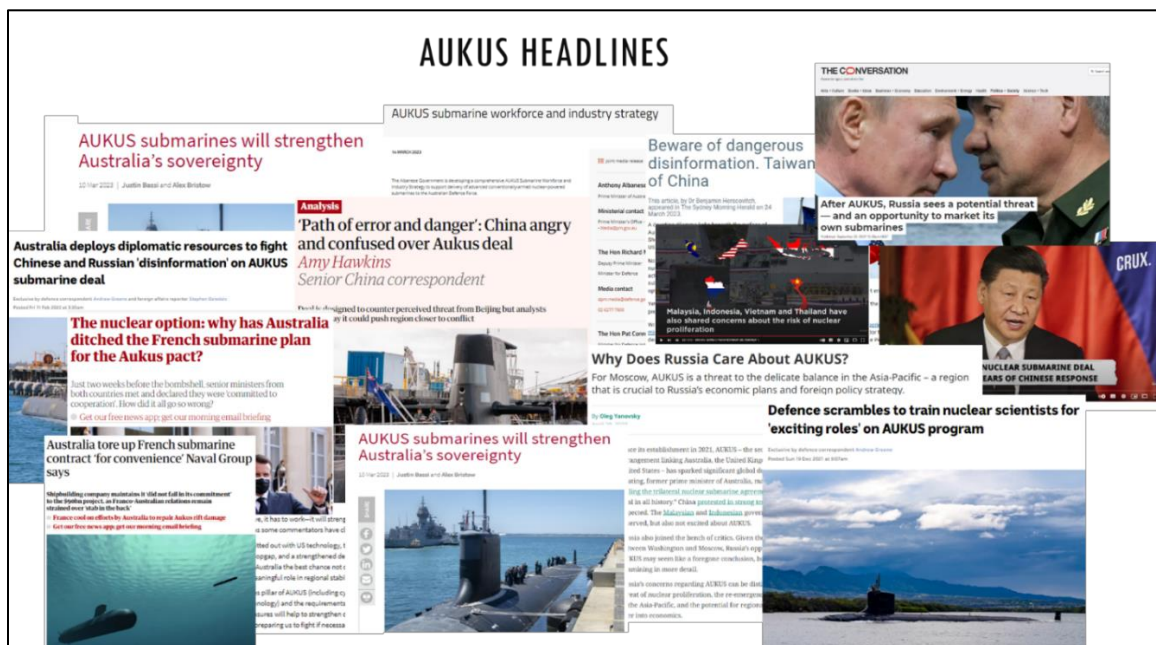


Figure 3: Adversarial Narrative Articles

Some headlines were seemingly positive such as 'AUKUS submarines will strengthen Australian sovereignty.'¹⁹ However, there were various articles that appeared very aggressive such as 'Path of Error and Danger: China Angry and confused over [AUKUS] deal.'²⁰

¹⁹ ASPI Strategist 10 Mar 2023, AUKUS submarines will strengthen Australia's sovereignty <<https://www.aspistrategist.org.au/aucus-submarines-will-strengthen-australias-sovereignty/>>

²⁰ The Guardian Thu 16 Mar 2023, 'Path of error and danger': China angry and confused over Aukus deal. <<https://www.theguardian.com/world/2023/mar/16/outrage-confusion-china-reaction-aukus-deal>>

There were also some that were relatively negative such as ‘after AUKUS Russia sees a potential threat.’²¹ Several of the articles showed concern such as ‘why does Russia care about AUKUS?’²² In addition, certain articles were based around political views including ‘the nuclear option: why has Australia ditched the French Submarine?’²³

Numerous researched articles appeared condemning towards Australia like ‘Australia tore up French contract for convenience.’²⁴ Finally, various articles were optimistic such as ‘Defence scrambles to train nuclear scientists for ‘exciting roles’ on AUKUS program.’²⁵

In summary, the Research Project Team found that at first glance, it is often difficult to determine if media articles are factual, contain misinformation, disinformation or malinformation, or a combination of all the above, and quite often there were articles which contradicted each other despite the appearance of being from reputable sources.

Research

Although not exhaustive, research conducted into the AUKUS Security Partnership included seventy articles across forty-seven reputable media sources. A summary of research is demonstrated in Figure 4 below.

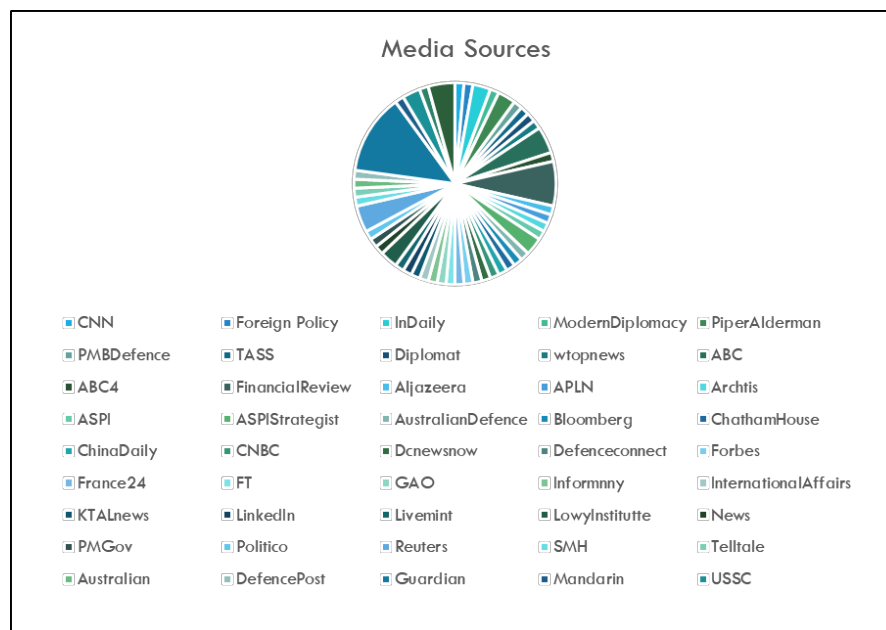


Figure 4: AUKUS Case Study Research

²¹ The Conversation September 23, 2021, After AUKUS, Russia sees a potential threat — and an opportunity to market its own submarines. <https://theconversation.com/after-aukus-russia-sees-a-potential-threat-and-an-opportunity-to-market-its-own-submarines-168374>

²² The Diplomat April 29, 2023, Why Does Russia Care About AUKUS? <https://thediplomat.com/2023/04/why-does-russia-care-about-aukus/>

²³ The Guardian Sat 18 Sep 2023, The nuclear option: why has Australia ditched the French submarine plan for the Aukus pact? <https://www.theguardian.com/australia-news/2021/sep/18/the-nuclear-option-why-has-australia-ditched-the-french-submarine-plan-for-the-aukus-pact>

²⁴ The Guardian Wed 29 Sep 2023, Australia tore up French submarine contract ‘for convenience’ Naval Group says, <https://www.theguardian.com/australia-news/2021/sep/29/australia-tore-up-french-submarine-contract-for-convenience-naval-group-says>

²⁵ ABC News Sun 19 Dec 2021, Defence scrambles to train nuclear scientists for ‘exciting roles’ on AUKUS program. <https://www.abc.net.au/news/2021-12-19/defence-staff-studying-nuclear-science-aukus-program/100710264?>

When the Research Project Team reviewed this information, it became apparent that the most common keywords included 'China' and 'Russia' which implies an element of foreign influence, and points towards misinformation. Overall, there was a great number of more negative than positive articles and it appeared that most were primarily aimed to sway the reader in many different directions. The research showed that most of the articles analysed contained some aspects of misinformation, disinformation or malinformation.

This also highlighted the fact that if the reader only considers the headlines and does not delve into the content, or does not consider multiple sources, it would be very likely that the reader would believe the headline hype to be the truth and therefore potentially misled.

The following three media articles provide examples of how embellished headlines can sway a reader.

Article Example #1 - Misinformation

The nuclear option: why has Australia ditched the French submarine plan for the Aukus pact?

Just two weeks before the bombshell, senior ministers from both countries met and declared they were 'committed to cooperation'. How did it all go so wrong?

● [Get our free news app; get our morning email briefing](#)



Figure 5: The nuclear option: why has Australia ditched the French submarine plan for the AUKUS pact?

This article was based around the AUKUS deal and included misinformation about why GoA made its decision, and what led to AUKUS being the preferred option for Australian submarine acquisition.

Additional information researched included a statement that the French could deliver a nuclear solution if Australia wanted one however, cancelling the Diesel-Electric French option in preference for the AUKUS nuclear option gave the Government a reason that the public could understand, even though this was misleading.

Article Example #2 - Disinformation



Figure 6: Path of error and danger: China angry and confused over AUKUS deal.

This article was based around the opinion of China's Foreign Ministry spokesperson and is an example of disinformation. The article talks about how the 'allies' namely Australia, UK and US are heading down a path of error and danger which could be read as antagonistic and inflammatory. The article further discusses that these three countries are fueling an arms race, including the assertion that nuclear weapons are an element of the AUKUS deal.

The acquisition and use of NPS however, does not imply the acquisition and deployment of nuclear weapons, hence the determination that this article contains disinformation.

Article Example #3 - Malinformation



Figure 7: Australia tore up French submarine contract 'for convenience' Naval Group says.

This article demonstrates malinformation and is intended to portray GoA in a negative light, and for *Naval Group* to appear as the victim, stating they [*Naval Group*] had done nothing wrong and further citing the consequences and impact to the company and to France. The article uses quotes such as '*Australian Navy says it was extremely satisfied that performance of the French submarine was excellent.*'

AUKUS Case Study Summary

Throughout the Research Project Team's research and analysis, it became evident that kinetic and non-kinetic threats need to be dealt with differently. Non-kinetic threats, in the context of adversarial narratives, are considered to involve persuasion, perception, and confidence which arguably can be more dangerous than a kinetic threat.

'Social Media' is emerging as a non-kinetic threat due to when 'factual' information is spread, it can be perceived as fiction or be used in a misleading or damaging way. It is often difficult to identify this threat and quantify the damage it causes.

This threat is not yet fully recognised or acknowledged and further, how to respond or defend against this emergent threat is yet to be determined. While historically, adversarial narratives can be equated to propaganda used during war, the proliferation of social media makes the threat more immediate and much more powerful.

Based on the Research Project Team's analysis, it was concluded that the dissemination of adversarial narratives through social media mechanisms can dramatically impact the growth, credibility, and stability of the Defence Industry in Australia.

To better understand how this threat could be managed by the Defence Industry in the future, the Research Project Team conducted a literature study on how the Cyber threat was managed, and how this threat could be compared to the adversarial narrative problem.

In addition, the Research Project Team noted that AI is a complicating and compelling factor in the delivery of, and response to, adversarial narratives. The team therefore conducted analysis into the use of AI in the media, specifically to determine whether AI could be part of the threat or potentially a solution.

Cyber Focus Area

The Australian Defence Industry plays a crucial role in countering adversarial cyber-attacks against Australia. Through collaborative efforts with GoA agencies, private sector partnerships, and research institutions, the Industry focuses on developing advanced cybersecurity technologies, conducting threat assessments, and enhancing the resilience of critical infrastructure.

By investing in cutting-edge capabilities and fostering a cyber-ready workforce, the Australian Defence Industry contributes to safeguarding the Nation's digital landscape from emerging cyber threats. As stated by the Australian Industry Group, 'the intelligence services of foreign governments present an enduring and serious espionage and foreign interference threat to Australia and Australian Defence Industry. State-sponsored espionage operations, particularly in the cyber realm, are often extremely well resourced and sophisticated, using high level and complex tools and capabilities.'²⁶

Problem Statement

The 2020 Defence Strategic Update detailed the deteriorating nature of Australia's strategic environment and the contributing role of cyber capabilities, as cyber threats are increasing in sophistication and scale. 'Cyber has emerged as a recognized warfighting domain and cyber warfare will be a critical component of future conflict.'²⁷

This was re-iterated by the Australian Industry Group in 2021, where they noted that: 'The intelligence services of foreign governments present an enduring and serious espionage and foreign interference threat to Australia and the Australian Defence industry with State-sponsored espionage operations, particularly in the cyber realm, are often extremely well resourced using high level and complex tools and capabilities.'²⁸

'Cyber and Information Warfare (IW), has now emerged as a recognized warfighting domain, with cyber warfare including IW being a critical component of conflicts across the world.'²⁹ Cyberspace has become a battleground as seen in Russia's use of malware designed to destroy data and preventing computers booting in Ukraine, resulting in Ukrainian Government officials acknowledging they are 'fighting a dual war – one on the ground and one in the digital realm.'³⁰

²⁶ The Australian industry group, 'Working securely with Defence, A guide to the Defence Industry Security Program', 2021, <<http://www.aigroup.com.au/sectors-and-advocacy/Defence/working-securely-with-defence/>>

²⁷ Australian Defence Department 2020, *Defence Strategic Update*

²⁸ The Australian industry group, 'Working securely with Defence, A guide to the Defence Industry Security Program', 2021, <<http://www.aigroup.com.au/sectors-and-advocacy/Defence/working-securely-with-defence/>>

²⁹ Wilson, G, 2023, *Information Warfare: what is it, and why should we care*, <Information Warfare: what is it, and why should we care? | The Cove (army.gov.au)>

³⁰ The Organisation for Economic Co-Operation and development (OECD) November 2022, *Disinformation and Russia's war of aggression against Ukraine* <<http://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/>>

GoA is actively engaged in steering the Nation's cybersecurity efforts. With a comprehensive strategy in place, it involves collaborating closely with the Defence Industry to ensure a unified and robust defense against cyber threats. This partnership extends to policy development, information sharing, and joint initiatives aimed at enhancing the Nation's cybersecurity posture.

Such initiatives include, however are not limited to;

- GoA committing in 2020 to invest AUD1.67 billion over 10 years to ensure Australia is cyber secure.
- Research and Development (R&D) tax incentive: a refundable tax offset (aggregate revenue under AUD20 million).
- GoA has introduced the Defence Industry Security Program (DISP) providing a framework for all Australian Defence companies in terms of commonality of expected norms to adhere to when working with DOD.
- REDSPICE Program: AUD5 billion for industry under a program that aims to triple the Australian Signals Directorate's (ASD) cyber security capability and double its cyber hunt activities.
- Cyber Security Skills Partnership Innovation Fund: AUD70 million to upskill and diversify staff in cyber security.
- ADF Cyber Gap Program: AUD41 million program offering financial support, mentoring and Defence work experience opportunities for cyber students.³¹

Through Government's coordinated approach of proactively collaborating with Defence Industry, there is a cohesive framework that both addresses the now of protecting Australia's digital infrastructure, as well as aiming to achieve what is required to combat the evolving levels of various national cyber challenges.

Understanding the Threat

What was not clear from the Research Project Team's literature review is how Australia as a nation is addressing adversarial narratives and Information Manipulation (IM). Due to IM being relatively cheap, requiring minimal technology requirements and easy to experiment with, it has allowed for a substantial uptake of threat actors utilising this deceptive apparatus, including through the modification and specific use of threat actors manipulating visual content, AI bots, trolling, account takeovers and search engine manipulation.

Because of this, Academia has been researching this matter with Oxford University's internet institute finding that IM has become a common strategy, with more than 93% of the countries surveyed seeing IM deployed via cyber as part of political communication using human accounts, used bot accounts, and used hacked or stolen accounts.³²

³¹ (Australian Government, Australia's cyber-security-strategy-2020.pdf)

³² Bradshaw, S 2021, Social media manipulation by political actors and industrial scale problem – Oxford report, accessed May 2023, <<https://www.ox.ac.uk/news/2021-01-13-social-media-manipulation-political-actors-industrial-scale-problem-oxford-report>>.

To better understand the threats posed by the expanding realm of IW, specifically its use in Australia, in 2002 GoA established the Select Committee on 'Foreign interference through social media'. The select committee was told by a cross section of Australian experts that foreign interference is now Australia's principal national security threat, which risks significantly undermining our values, freedoms, and way of life.

The committee further acknowledged that 'various regimes continue to pose an unacceptable risk to democratic societies such as Australia through targeted online disinformation campaigns.'³³

In July 2023, the Select Committee tabled 17 recommendations for Government to consider and implement ranging from promoting the digital literacy in developing countries in the Indo-Pacific region to establishing a national security technology office within the Department of Home Affairs.³⁴

Cyber Focus Area Summary

IW is considered the dominant military doctrine of adversarial nations who believe that the perceptions of their adversaries are central to current and future conflict(s); that to win in this domain has the potential to make victory in combat significantly easier. These nations do not recognise IW as being confined to war but consider it an essential prerequisite to set conditions in their favour.³⁵

GoA, particularly DOD must begin to understand what IW is and how to practice IW in a manner consistent with our laws and values. However, this cannot be confined to Government alone and it is essential that whole-of-government collaborates with Defence Industry to conduct effective IW campaigns that promote our national interests while simultaneously attempting to neutralise adversary efforts in the same space.

As IW has increased exponentially due to its minimal reliance of advanced technology, it has also meant that the most logical way forward is for threat actors to maximise the utilisation of the next technology advancement – AI. The joint philosophy of causing as much disruption as possible through the lens of IW, as well as the adoption of AI has meant both have now become closely intertwined, forming a complex landscape where technology, politics, and security intersect. AI now plays a pivotal role in IW enabling sophisticated tools for IM, and cyber-attacks. From deep fake technology to automated propaganda, AI amplifies the impact of IW, challenging traditional notions of truth and trust.

³³ Parliament of Australia July 2023, Senate Select Committee on foreign Interference through Social Media, APH, Canberra

³⁴ Parliament of Australia July 2023, Senate Select Committee on foreign Interference through Social Media, APH, Canberra

³⁵ Wilson, G, 2023, *Information Warfare: what is it, and why should we care*, <Information Warfare: what is it, and why should we care? | The Cove (army.gov.au)>

AI Focus Area

The Research Project Team's report delved into the landscape of AI and its relationship with adversarial narratives, aiming to provide a comprehensive understanding of AI's capabilities, the associated threats, the need for collaboration, ethical considerations, and actionable steps for the future.

Background

AI represents the simulation of human intelligence in machines, enabling reasoning, learning, and problem-solving. It has evolved significantly over the years, impacting various domains, including the media and security.³⁶

Research

To investigate the AI relationship with adversarial narratives, the Research Project Team initiated a dialogue with two advanced AI models - Google's *Bard* and *ChatGPT-4*, asking both platforms to answer the research question. The responses from each interrogation are detailed at Appendix 1 and Appendix 2.

Secondly, AI was utilised to inform research on the AUKUS Cast Study. This initial interrogation served as the foundation for the research and by engaging AI entities, the Research Project Team was able to glean insights into AI's understanding of this complex issue.

The insights derived from these interactions guided further research and analysis, enabling a deeper probe into the multifaceted relationship between AI and adversarial narratives, with the goal of better understanding the implications and challenges posed by AI in shaping public perception and trust in Defence acquisition and security contexts.

Google Bard AI - Negative Text

- The AUKUS submarine deal is a waste of money that could be better spent on other priorities, such as healthcare or education.
- The deal will increase tensions in the region and make it more likely that there will be a conflict between Australia and China.

³⁶Turing, A. M. (1950). Computing machinery and intelligence. *Mind*, 59(236), 433-460. McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (1956). A proposal for the Dartmouth summer research project on artificial intelligence. Newell, A., & Simon, H. A. (1961). GPS, a program that simulates human thought. NRC (U.S.). (1973). *Artificial Intelligence: A RAND Perspective*. Buchanan, B. G., & Shortliffe, E. H. (Eds.). (1984). *Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project*. Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). *From data mining to knowledge discovery in databases*. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444. Radford, A., Narasimhan, K., Salimans, T., & Sutskever, I. (2018). Improving Language Understanding by Generative Pre-trained Transformers. Thrun, S., Montemerlo, M., Dahlkamp, H., Stavens, D., Aron, A., Diebel, J., ... & Thayer, S. (2006). Stanley: The robot that won the DARPA Grand Challenge.

- The deal will set a dangerous precedent for other countries and could lead to a nuclear arms race in the Indo-Pacific.
- The deal is not in Australia's national interest, and it will make the country more vulnerable to attack.
- The deal is a betrayal of France, which was [one of] Australia's traditional partners.
- The deal will damage Australia's reputation in the world and make it more difficult to build trust with other countries.

These are just some of the negative arguments that have been made against the AUKUS submarine deal by one AI platform. It is important to note that there are also many people who support the deal, and who believe that it is necessary to protect Australia's security in the face of the growing threat from China.

Google Bard AI - Positive Text

- The AUKUS submarine deal will significantly enhance Australia's capabilities, making the country more secure in the face of the growing threat from China.
- The deal will create new jobs and opportunities in Australia's industry, supporting economic growth and prosperity.
- The deal will strengthen Australia's ties with the United States and the United Kingdom, two of its closest allies.
- The deal will send a strong message to China that Australia is committed to defending its sovereignty and interests.
- The deal will help to promote stability and security in the Indo-Pacific region.

These are just some of the positive arguments that have been made in favor of the AUKUS submarine deal through the interrogation of one AI platform. It is important to note that there are also many people who oppose the deal, and who believe that it is unnecessary or even dangerous.

Ultimately, the decision of whether to support the AUKUS submarine deal is a complex one, and there are valid arguments to be made on both sides. The AUKUS submarine deal is a major strategic development for Australia, and it is likely to have a significant impact on the country's capabilities and its role in the Indo-Pacific region. It is important to weigh all the arguments carefully before making a decision, and AI is just one source of information which can be utilised.

AI Focus Area – Preliminary Findings

AI Capabilities: AI has the potential to revolutionise various industries by simulating human intelligence, particularly through deep learning algorithms and neural networks. It can think, reason, learn, and problem-solve, making it a powerful tool for a wide range of applications.³⁷

³⁷ "Deep Learning" by Ian Goodfellow, Yoshua Bengio, and Aaron Courville. "Artificial Intelligence: A Guide to Intelligent Systems" by Michael Negnevitsky. Mustafa Suleyman & Yuval Noah Harari -FULL DEBATE- What does the AI revolution mean for our future? - YouTube

Adversarial Narratives and Threats: Adversarial narratives can have significant consequences, including misinforming public opinion, eroding trust in defence institutions, and potentially leading to flawed strategic decisions. AI plays a role in amplifying these threats by generating convincing and personalized narratives at scale. However, quantifying the exact impact of AI on Defence Industry remains a challenge.^{38 39}

The Need for Collaboration: Collaborative efforts involving multiple stakeholders, including the Defence Industry, Academia, and Government, are crucial to effectively address AI-related challenges. A strategic and multi-sector approach is essential to harness AI's potential and mitigate its threats.⁴⁰

Ethical Considerations: When employing AI in defence and security contexts, ethical considerations are paramount. Key principles include truthfulness, transparency, data privacy, accountability, avoiding bias, ensuring proportionality, maintaining human oversight, being cautious of emotional manipulation, adhering to international norms, and upholding democratic values.^{41 42}

Actionable Steps and Future Directions: Implementing best practices and ethical guidelines is essential for effectively utilising AI in defence and security. Understanding potential issues and planning for ethical action is critical to navigate the evolving landscape of AI and adversarial narratives.⁴³

Urgency for Action: The research underscores the urgency for rapid action in addressing AI-related challenges. Delays in countering false narratives or ensuring ethical AI practices could have significant consequences for security and public perception.⁴⁴

Subjectivity in AI Research: The research acknowledges that AI research can be subjective, potentially confirming preconceived notions rather than revealing objective truths. This highlights the need for careful analysis and ethical considerations in AI development and deployment.⁴⁵

These findings collectively emphasize the complex and multifaceted nature of AI and adversarial narratives in the Defence and security domains. They call for a nuanced and collaborative approach that combines technological innovation with ethical considerations to navigate the challenges and opportunities presented by AI.

³⁸ LikeWar: The Weaponization of social media" by P. W. Singer and Emerson T. Brooking "The Death of Expertise" by Tom Nichols

³⁹ "Superintelligence" by Nick Bostrom. "Our Final Invention" by James Barrat

⁴⁰ Team Geek" by Ben Collins-Sussman, and "The Phoenix Project" by Gene Kim

⁴¹ Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines.

⁴² "AI Ethics" by Mark Coeckelbergh. "Data Ethics" by Luciano Floridi

⁴³ The New Digital Age" by Eric Schmidt and Jared Cohen. "The Second Machine Age" by Erik Brynjolfsson and Andrew McAfee

⁴⁴ The Black Box Society" by Frank Pasquale. "The Age of Em" by Robin Hanson

⁴⁵ "Weapons of Math Destruction" by Cathy O'Neil. "Ethics of Artificial Intelligence" by Nick Bostrom and Eliezer Yudkowsky

AI Focus Area – Summary

AI's Dual Role:

AI is a powerful tool that serves a dual purpose in narrative formation. On one hand, it has the capacity to rapidly generate narratives, offering a valuable asset in information dissemination. However, the creation of nuanced counter-narratives often necessitates human involvement to provide essential context and nuanced insights. In the realm of Defence and security, AI wields a significant influence on narrative formation presenting both opportunities and challenges.

AI's ability to generate adversarial narratives carries the potential to distort public opinion, undermine trust in defence institutions, and trigger adverse consequences such as reduced funding and strained alliances. Yet, quantifying the extent of this AI threat remains a complex task, and one that demands precision.⁴⁶

⁴⁶ Future Crimes" by Marc Goodman for understanding the scope of potential issues.. "Designing Your Life" by Bill Burnett and Dave Evans for a methodology in action planning

Findings

The Research Project Team conducted thorough research and analysis into the research topic, utilising the AUKUS Case Study and the focus areas of Cyber and AI. Research was primarily focused on social media outlets; however, traditional media sources were also considered. To validate and ensure the research and analysis was contemporary and accurate, the Research Project Team conducted several semi-structured qualitative interviews with media thought leaders to gain their insights into the current contested IE; and to validate the research and analysis conducted, ensuring it was contemporary, accurate and aligned with industry thinking.

Although not exhaustive, the Research Project Team identified the following seven key findings:

1. **There are any media sources of influence on Defence Industry.** Despite the research being focused on Social Media mechanisms, and further focused primarily on foreign influence and actors, the Research Project Team acknowledges that there are many other media sources of influence which may affect the Defence Industry in varied ways. Specifically, it is not only foreign influence which affects the industry but also Australia's own mainstream media outlets, to also include internal Defence and Defence Industry reporting; both of which can affect perception and decision making within the Industry.
2. **Collectively, we do not fully comprehend the threat.** Evidenced by the lack of available literature to address this concern, it remains clear that Australia wholistically does not yet fully comprehend the extent of the threat from adversarial narratives, and the mechanisms used for their delivery. Although the threat from Cyber, AI and foreign influence narratives are becoming well-known to senior Government and Defence officials, there is a lack of contemporary information available to assess the threat on a deep level, and even less to devise a solution. What is known however, is that adversarial narratives are having, and will continue to have, an impact on the growth, credibility, and stability of the Defence Industry.
3. **Social Media: persuasion and perception to undermine reality.** Social Media in its many forms has an ability to rapidly disseminate information but concerningly, it is how information is portrayed and how facts are manipulated and often skewed into fiction that presents the more compelling threat. Having an ability to identify these threats in an agile and responsive way has been found to be difficult to achieve, and more difficult to counter.
4. **Difficult to determine if media articles are factual.** Despite researching and analysing media articles from known reliable sources, or those which appeared to come from reputable sources, the Research Project Team found that numerous articles contained misinformation, disinformation, or malinformation and in some cases a cross section of all three. It was therefore concluded that to the average reader it is very difficult to ascertain if media articles are factual and if they can be trusted.

5. **State-sponsored [Foreign] information campaigns designed to push their Nation's narrative.** State sponsored IM agencies are tasked to push their Nation's narrative which in turn can undermine another nation's [public] trust, thereby amplifying uncertainty in public institutions and discrediting authority and decision-making bodies. IM campaigns often rely heavily on made-up facts which can incite conspiracies, affecting a targeted nation's institutional credibility. As stated by an industry expert, 'misinformation and disinformation frequently get footholds when fear is involved, and there is promotion of ignorance; and a laziness around getting real information.'⁴⁷ Defence Industry is not immune to these targeted threats from foreign State actors.
6. **The public is confronted with large volumes of increasingly conflicting information.** The general public is confronted with large volumes of increasingly conflicting information, which demands a greater effort to navigate to establish reality and truth which can result in ill-informed biases and opinions. Through these ill-informed biases, a misinformed or influenced public can lead to the erosion of trust in Government institutions, including Defence and Defence Industry.
7. **AI narratives enable real-time generation of complex and shaped stories.** There is a substantial body of research on AI's role in information dissemination, including creating and propagating disinformation, malformation, and misinformation; AI amplifies the threat of adversarial narratives by the rapid generation and dissemination of convincing narratives which are often personalized and targeted. As cited by NATO's Strategic Communication Centre in 2023, 'the fast pace at which AI can generate and disseminate information necessitates an equally rapid response... delays in countering false narratives can result in irreversible damage... emphasizing the need for rapid, yet accurate, identification and mitigation of disinformation campaigns.'⁴⁸ Further, the Research Project Team identified that the extent to which AI can damage the Defence Industry is not yet fully quantified.

⁴⁷ Lynne Duckham, OAM, Industry Expert, interview October 2023

⁴⁸ NATO's Strategic Communications Centre, 2023

Recommendations

Based on the Researched Project Team's in-depth research and analyst, case study, focus area assessment, literature reviews and validation interviews with industry experts, eight recommendations have been drawn from the key findings.

1. **Recognition – understand and acknowledge the threat.** Despite the problem being well-known to senior Government, Defence and Industry officials, the threat from adversarial narratives is not fully understood nor has it been adequately acknowledged. Akin to the emergence of Cyber based threats, it took many years before Government openly acknowledged the threat was real, contemporary, and was having a marked impact not only on day-to-day life, but on key activities and decisions within Defence. Adversarial narratives, and their propagation using Cyber and AI is the equivalent to the threat posed by cyber-attacks in the 2010+ period. This emerging concern needs to be addressed through investment across Government and Industry.
2. **A better understanding of the actors: Capability + Intent = Threat.** Collectively, Government and Industry need to better understand the actors behind the threat of adversarial narratives. A deeper comprehension of the actors will yield a more robust understanding of their capabilities. Are the actors state-sponsored, individuals, or are they politically motivated groups? What these actors are trying to achieve is the other question which needs to be addressed; a knowledge of their intent along with their capabilities will assist with determining the threat posed and will also provide a counterview into adversary vulnerabilities.
3. **More cognisance of the threat vectors and mechanisms.** Analysis of traditional [foreign] media reporting is no longer sufficient to determine the threat posed by actors intending harm to the Defence Industry. Emerging mechanisms including Cyber and AI are rapidly enhancing the adversary's ability to influence the public, and target Government and Industry directly. Establishing counter-cyber principles and capabilities is essential to the ability to counter and respond to the ongoing threat. AI is further complicating the issue and there is an immediate need for real-time AI monitoring and a capability to respond.
4. **Industry needs to proactively highlight skills and capability offerings.** Australia possesses a great deal of sovereign capability within the Defence Industry and these capabilities should be openly acknowledged and celebrated. Sovereign capability presents an opportunity not only for Industry, but also for Defence. A symbiotic relationship between DOD and Industry will further create opportunity however, there needs to be increased openness and transparency from GoA regarding Defence acquisitions, allowing Industry to better demonstrate relevant capability – 'we need to support the preservation of trust in Australian institutions.'⁴⁹

⁴⁹ Damien Spry, Adjunct Research Fellow, UniSA and Social Influence researcher at DSTG, interview, October 2023

6. **Use the media to achieve positive influence.** Most Defence Industry SMEs have something unique to offer Defence, which would also be of great benefit; but that story needs to be told independently. SME brand marketing needs to be more visible and actively promoted. Defence Industry should not simply wait for and react to adversarial narratives, but instead be on the front foot and proactively tell good news stories, and the media is a prime opportunity to achieve this – ‘we need to preserve an independent, diverse and professional media, and support a healthy information ecosystem where different views are accepted but within regulatory frameworks.’⁵⁰
7. **Education, vigilance, and responsiveness.** Education is paramount and a key recommendation from the Research Project Team. Cognitive Immunity training is accessible, but needs additional funding, visibility and promotion throughout Defence Industry and DOD. Industry advocacy organisations across Australia already provide guidance, support, and education however, with further resourcing and funding, could make a marked difference in combating the threat posed by adversarial narratives. Not only is this concern one for the Government to address but equally, private enterprise also needs to contribute to the cause through improved company policies and procedures, and investment.
8. **Defence Industry needs to collaborate.** The final recommendation, and perhaps the most important, is that Defence Industry needs to collaborate; the Industry needs to work toward cohesion across Defence, Academia and Government more broadly. A common front between the Primes and SMEs is fundamentally important and could include aligned media strategies and engagement as a starting point. Specifically, AI needs additional investment and recognition, and this could be achieved through dedicated conferences and summits to address the concerns raised from a cohesive standpoint.

⁵⁰ Damien Spry, Adjunct Research Fellow, UniSA and Social Influence researcher at DSTG, interview, October 2023

Conclusion

Adversarial narratives in all their forms have, and continue to have, a negative influence on Australia's Defence Industry. The Research Project Team has identified these threats as real and immediate, yet not fully understood.

We need a collective and cohesive approach by Industry, Government and Academia to fight this systemic issue. The Defence Industry is encouraged to seek a united approach to countering adversarial narratives, with Primes and SMEs aligning media and engagement strategies as a starting point. The team also recommends that Industry invests in a series of dedicated conferences and summits as a recognition of the immediate threat of AI, and to better understand its potential to counter adversarial narratives.

To help resolve the issue and avert further risk to the Defence Industry, our recommendations have been presented for consideration, and where applicable and appropriate, for implementation.

References

1. Decker, B, 2019, Adversarial Narratives: A New Model for Disinformation; The Global Disinformation Index , <<https://www.disinformationindex.org/research/2019-4-1-adversarial-narratives-a-new-model-for-disinformation/>>
2. How to identify misinformation, disinformation and malinformation, 2022, Canadian Centre for Cyber Security
3. How to identify misinformation, disinformation and malinformation, 2022, Canadian Centre for Cyber Security
4. How to identify misinformation, disinformation and malinformation, 2022, Canadian Centre for Cyber Security
5. Wilson, G, 2023, Information Warfare: what is it, and why should we care, <Information Warfare: what is it, and why should we care? | The Cove (army.gov.au)>
6. The Cybersecurity and Infrastructure Security Agency (CISA), information_manipulation_infographic_508.pdf
7. How to identify misinformation, disinformation and malinformation, 2022, Canadian Centre for Cyber Security
8. The Real Story of Fake News, nd, Merriam-Webster
9. Human Rights Commissioner Lorraine Finlay, 2023, Why Misinformation Bill risks Freedoms it Aims to Protec, The Australian, published Thursday 24th August 2023
10. Leshner, M., H. Pawelec and A. Desai, 2022, Disentangling untruths online: Creators, spreaders and how to stop them, OECD Going Digital Toolkit Notes, No. 23, OECD Publishing, Paris
11. Buckmaster L, Wils, T, nd, Responding to fake news, Parliament of Australia
12. Ebbott, E, Saletta, M, Stearne, R, Webb, B, Dowling, M, Farina, M, Young, G, Job, P, 2021, Understanding Mass Influence, Edith Cowan University, Macquarie University, University of Adelaide, University of Melbourne, University of New South Wales
13. Meta 2023, Meta response to the Australian disinformation and misinformation industry code – January – December 2022
14. Leshner, M., H. Pawelec and A. Desai, 2022, Disentangling untruths online: Creators, spreaders and how to stop them, OECD Going Digital Toolkit Notes, No. 23, OECD Publishing, Paris
15. Edelman 2023, Edelman Trust Barometer – Australian Report
16. Hollingworth 2023, ADF Chief warns of ‘truth decay’ in talk touching on AI and disinformation, Defence Connect, 22 September 2023
17. Price, M, Australia’s Defense Industry Minister: The importance of AUKUS and a strong economy, Defense News, 6 December 2021
18. Combating Disinformation through Collaborative Research, Department of Defence Media Centre, 22nd December 2022 , <<https://www.dst.defence.gov.au/news/2022/12/22/combating-disinformation-through-collaborative-research>>
19. ASPI Strategist 10 Mar 2023, AUKUS submarines will strengthen Australia’s sovereignty <<https://www.aspistrategist.org.au/aukus-submarines-will-strengthen-australias-sovereignty/>>
20. The Guardian Thu 16 Mar 2023, ‘Path of error and danger’: China angry and confused over Aukus deal. <<https://www.theguardian.com/world/2023/mar/16/outrage-confusion-china-reaction-aukus-deal>>
21. The Conversation September 23, 2021, After AUKUS, Russia sees a potential threat — and an opportunity to market its own submarines. <https://theconversation.com/after-aukus-russia-sees-a-potential-threat-and-an-opportunity-to-market-its-own-submarines-168374>
22. The Diplomat April 29, 2023, Why Does Russia Care About AUKUS? <https://thediplomat.com/2023/04/why-does-russia-care-about-aukus/>
23. The Guardian Sat 18 Sep 2023, The nuclear option: why has Australia ditched the French submarine plan for the Aukus pact? <https://www.theguardian.com/australia-news/2021/sep/18/the-nuclear-option-why-has-australia-ditched-the-french-submarine-plan-for-the-aukus-pact>
24. The Guardian Wed 29 Sep 2023, Australia tore up French submarine contract ‘for convenience’ Naval Group says, <https://www.theguardian.com/australia-news/2021/sep/29/australia-tore-up-french-submarine-contract-for-convenience-naval-group-says>
25. ABC News Sun 19 Dec 2021, Defence scrambles to train nuclear scientists for ‘exciting roles’ on AUKUS program. <https://www.abc.net.au/news/2021-12-19/defence-staff-studying-nuclear-science-aukus-program/100710264?>
26. The Australian industry group, ‘Working securely with Defence, A guide to the Defence Industry Security Program’, 2021, <<http://www.aigroup.com.au/sectors-and-advocacy/Defence/working-securely-with-defence/>>

27. Australian Defence Department 2020, Defence Strategic Update
28. The Australian industry group, 'Working securely with Defence, A guide to the Defence Industry Security Program', 2021, <<http://www.aigroup.com.au/sectors-and-advocacy/Defence/working-securely-with-defence/>>
29. Wilson, G, 2023, Information Warfare: what is it, and why should we care, <Information Warfare: what is it, and why should we care? | The Cove (army.gov.au)>
30. The Organisation for Economic Co-Operation and development (OECD) November 2022, Disinformation and Russia's war of aggression against Ukraine < [http:// www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/](http://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/)>.
31. (Australian Government, Australia's cyber-security-strategy-2020.pdf)
32. Bradshaw, S 2021, Social media manipulation by political actors and industrial scale problem – Oxford report, accessed May 2023, <<https://www.ox.ac.uk/news/2021-01-13-social-media-manipulation-political-actors-industrial-scale-problem-oxford-report>>.
33. Parliament of Australia July 2023, Senate Select Committee on foreign Interference through Social Media, APH, Canberra
34. Parliament of Australia July 2023, Senate Select Committee on foreign Interference through Social Media, APH, Canberra
35. Wilson, G, 2023, Information Warfare: what is it, and why should we care, <Information Warfare: what is it, and why should we care? | The Cove (army.gov.au)>
36. Turing, A. M. (1950). Computing machinery and intelligence. *Mind*, 59(236), 433-460. McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (1956). A proposal for the Dartmouth summer research project on artificial intelligence. Newell, A., & Simon, H. A. (1961). GPS, a program that simulates human thought. NRC (U.S.). (1973). Artificial Intelligence: A RAND Perspective. Buchanan, B. G., & Shortliffe, E. H. (Eds.). (1984). Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project. Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444. Radford, A., Narasimhan, K., Salimans, T., & Sutskever, I. (2018). Improving Language Understanding by Generative Pre-trained Transformers. Thrun, S., Montemerlo, M., Dahlkamp, H., Stavens, D., Aron, A., Diebel, J., ... & Thayer, S. (2006). Stanley: The robot that won the DARPA Grand Challenge.
37. "Deep Learning" by Ian Goodfellow, Yoshua Bengio, and Aaron Courville. Artificial Intelligence: A Guide to Intelligent Systems" by Michael Negnevitsky. Mustafa Suleyman & Yuval Noah Harari -FULL DEBATE- What does the AI revolution mean for our future? - YouTube
38. LikeWar: The Weaponization of social media" by P. W. Singer and Emerson T. Brooking "The Death of Expertise" by Tom Nichols
39. "Superintelligence" by Nick Bostrom. Our Final Invention" by James Barrat
40. Team Geek" by Ben Collins-Sussman, and "The Phoenix Project" by Gene Kim
41. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines.
42. "AI Ethics" by Mark Coeckelbergh. "Data Ethics" by Luciano Floridi
43. The New Digital Age" by Eric Schmidt and Jared Cohen. The Second Machine Age" by Erik Brynjolfsson and Andrew McAfee
44. The Black Box Society" by Frank Pasquale. "The Age of Em" by Robin Hanson
45. "Weapons of Math Destruction" by Cathy O'Neil. "Ethics of Artificial Intelligence" by Nick Bostrom and Eliezer Yudkowsky
46. Future Crimes" by Marc Goodman for understanding the scope of potential issues.. "Designing Your Life" by Bill Burnett and Dave Evans for a methodology in action planning
47. Lynne Duckham, OAM, Industry Expert, interview October 2023
48. NATO's Strategic Communications Centre, 2023
49. Damien Spry, Adjunct Research Fellow, UniSA and Social Influence researcher at DSTG, interview, October 2023
50. Damien Spry, Adjunct Research Fellow, UniSA and Social Influence researcher at DSTG, interview, October 2023.

Appendix 1

Google Bard AI Research Question Response

Adversarial narratives are a type of disinformation that is designed to undermine public trust in an organization or government. They can be spread through a variety of channels, including social media, traditional media, and even word-of-mouth.

The defence industry is particularly vulnerable to adversarial narratives, as it is often seen as a symbol of government power and authority. Adversarial narratives can be used to sow doubt about the defence industry's capabilities, to undermine public support for military action, or to promote a particular political agenda.

There are a number of things that the defence industry can do to counter adversarial narratives. These include:

- Identifying and understanding the adversary. The first step in countering adversarial narratives is to understand who is behind them and what their goals are. This can be done by monitoring social media, traditional media, and other channels where adversarial narratives are being spread.
- Building a strong counter-narrative. Once the adversary has been identified, the defence industry can start to build a strong counter-narrative. This counter-narrative should be based on facts and should be presented in a clear and concise way.
- Distributing the counter-narrative. The counter-narrative needs to be distributed widely so that it reaches a large audience. This can be done through social media, traditional media, and other channels.
- Engaging with the public. The defence industry should also engage with the public to answer their questions and address their concerns. This can help to build trust and credibility and to counter the spread of adversarial narratives.
- Countering adversarial narratives is a complex and challenging task. However, by taking the steps outlined above, the defence industry can help to protect itself from the negative effects of disinformation.

Here are some additional tips for countering adversarial narratives:

- Be transparent and open about your activities.
- Use clear and concise language.
- Use visuals to help tell your story.
- Be consistent in your messaging.
- Be patient and persistent.

It is important to remember that there is no one-size-fits-all solution to countering adversarial narratives. The best approach will vary depending on the specific situation. However, by following the tips above, the defence industry can increase its chances of success.

Appendix 2

Chat GPT-4 Research Question Response

In a contested informational environment, the defense industry faces challenges in countering adversarial narratives that may aim to undermine its reputation, sow doubt, or spread misinformation. Here are some strategies the defense industry can employ to address this issue effectively:

1. *Proactive Communication*: Establish a strong and consistent communication strategy to disseminate accurate and timely information about the industry's activities, achievements, and contributions to national security. Regularly engage with the public, media, and stakeholders to build trust and credibility.
2. *Education and Awareness*: Conduct public awareness campaigns to educate the public about the defense industry's role, its importance in national security, and its commitment to ethical practices. This can help combat misconceptions and improve public understanding.
3. *Fact-Checking and Debunking*: Monitor and identify false or misleading narratives about the defense industry. Respond promptly with factual evidence and credible sources to debunk misinformation. Engage with independent fact-checking organizations to strengthen these efforts.
4. *Engage with Digital Platforms*: Collaborate with social media platforms and technology companies to identify and counter disinformation campaigns that target the defense industry. Implement measures to flag and report false information and collaborate on initiatives to improve online information integrity.
5. *Public-Private Partnerships*: Collaborate with academia, think tanks, and research institutions to conduct and publish objective studies on defense-related topics. Engaging in credible research can support the industry's positions and foster informed discussions.
6. *Crisis Management*: Develop a robust crisis communication plan to respond swiftly and effectively to emerging adversarial narratives or incidents. A well-prepared response can help mitigate the impact of negative information and protect the industry's reputation.
7. *Media Engagement*: Build positive relationships with journalists and media outlets to ensure accurate and balanced reporting on defense industry matters. Proactively provide information and expert insights to journalists, promoting fair and accurate coverage.
8. *Employee Advocacy*: Empower employees to be advocates for the industry. Educate them about the industry's values, activities, and contributions, so they can address misinformation and share positive narratives in their personal and professional networks.
9. *Transparency and Accountability*: Demonstrate transparency in operations and decision-making processes. Publicly disclose relevant information about projects, contracts, and partnerships to build credibility and dispel suspicions.

10. *Ethical Practices*: Uphold the highest ethical standards in all aspects of the industry's operations. Demonstrating a commitment to integrity and responsible behavior reinforces public trust.

11. *Engage in Dialogue*: Openly engage with critics and opponents to address concerns and misconceptions constructively. Respectful dialogue can foster understanding and potentially change adversarial perspectives.

By adopting a multifaceted approach that combines proactive communication, fact-checking, collaboration, and ethical conduct, the defense industry can better counter adversarial narratives and ensure accurate information prevails in the contested informational environment.